The Genger Case And The Delaware Supreme Court

Vicki Luoma, Minnesota State University, Mankato, USA
Milton Luoma, Metropolitan State University, St. Paul, USA
Penny Herickhoff, Minnesota State University, Mankato, USA

ABSTRACT

The Genger case, a recently decided case by the Delaware Supreme Court, involves the imposition of severe sanctions upon one party who erased unallocated free space on his computer after having made his computer available to a court-appointed digital forensics expert who had the opportunity to obtain a forensic image of any data on the computer thought to be relevant to the case. The expert did not image unallocated space, which was later erased by Genger's expert. If the results of this case are adopted as binding precedent in jurisdictions outside of Delaware, important implications arise regarding business practices related to electronic discovery. This paper concludes by offering recommendations on how businesses can best deal with the requirements set forth by the Delaware court and best practices for electronic discovery.

Keywords: The Genger Case and the Delaware Supreme Court; Unallocated Space and Electronic Discovery; Digital Forensics

INTRODUCTION

Few legal cases in the United States have had as much of an impact on the electronic discovery landscape as did the Zubulake case that led to a major revision in 2006 of the Federal Rules of Civil Procedure with respect to electronic discovery. However, the recent Genger case in a Delaware state court, where a judge imposed severe sanctions on a party for erasing unallocated or free space from a computer's hard disk *after* having made his computer available to a court-appointed digital forensics expert for examination, may well have as major an impact on electronic discovery practice. (Genger v. TR Investors, LLC, 2011) If the holding in the Genger case is widely adopted in jurisdictions outside of Delaware, the implications of that case for businesses of all types and sizes will have a significant influence on business practices. While the decision by the Delaware Supreme Court is binding only within the State of Delaware, other jurisdictions may very well find the holding and reasoning behind the holding persuasive enough to be adopted in those other jurisdictions. In this paper the specifics of the Genger case are examined with respect to electronic discovery and its impact on business practices in the event it becomes widely viewed in the United States as a valid precedent that should be followed in cases involving similar electronic discovery issues. The specific points of the case's electronic discovery issues are discussed followed by the implications for business should this case be adopted in all United States jurisdictions. Finally, the conclusions and recommendations focus on business practices rather than legal issues and offer guidance to management on the implications of the Genger case.

THE GENGER CASE

In 2011 the Delaware Supreme Court upheld severe sanctions levied by a Delaware state court trial judge against a litigant who intentionally erased data from the unallocated space on his computer and the company server after a status quo order had been issued. Sanctions are punishments that are levied against litigants or their attorneys for not following the court orders, particularly when a party has been guilty of spoliation of evidence, that is, when that party has destroyed evidence whether intentionally or accidentally. (Sedona Conference, 2007) If a court finds that a party is guilty of spoliation of evidence, then sanctions can vary from fines, attorney fees, costs, adverse-inference jury instructions or summary judgment. (Brady, 2010) The destruction in this case was deliberate, but was

the destruction knowingly in violation of the status quo order, and more importantly, should it ever be a violation of a general status quo order?

Deleted data can generally be recovered using proper forensic technology and knowledgeable forensic experts, but in the Genger case the court determined that Genger intentionally cleared the unallocated space with a wiping program. There are numerous relatively inexpensive but very effective wiping programs that can be used to erase as much or as little data as the user directs. In this case Genger was concerned about the possibility that fragments of unencrypted deleted data unrelated to the case at hand that might have been left in unallocated space, so on the advice of a technical expert, Genger used SecureClean, a wiping program that was used to erase only the unallocated space on his hard drive that might have contained file fragments. As soon as the opposing side discovered that this had occurred, they asked the court to reopen the settled case and find that Genger had violated the court's status quo order.

At the heart of the issue is whether a status quo order includes unallocated space on a computer without specifically mentioning it. Status quo orders are typically intended to maintain the situation as it is until further order of the court, or until the case is resolved. Normal status quo orders allow companies or individuals to continue in their normal business operations but do not allow them to do anything extraordinary. The pivotal question is whether this status quo order included the preservation of unallocated space or must there be a specific order including this space as an extraordinary request? Should future litigants ask for or expect the protection of unallocated space to be preserved on a hard drive in response to a status quo order? How can unallocated or free space be protected and is it feasible to do so? The answer to these questions could become the catalyst for drastic changes for companies, forensic experts, and lawyers.

Even though courts have not always consistently dealt with the issue of allocated versus unallocated space prior to the Genger case, court orders typically did not include the unallocated space without a specific order directing otherwise. (Brady, 2010). Key to resolving this issue is an understanding of what the unallocated space on a computer is and what it would encompass to protect that space from deletion.

DIGITAL STORAGE MEDIA UNALLOCATED SPACE

Simply stated, unallocated storage space on a computer's storage media, such as its hard drive, is space that is not currently used for active electronic file storage. As such, it is considered to be available to other files should the need for additional space arise in the event a file is modified or a new file needs storage space. Unallocated space, also known as free space, may possibly contain fragments of old files that have been previously deleted or fragments of files and programs temporarily stored in unallocated space by the computer's operating system. The reason unallocated space may contain file fragments is because when a file is deleted, the data is not erased. It is simply more efficient for the operating system to alter one single bit that indicates whether a given sector of storage space is currently in use by an active file or whether it is free for other use.

If a document is opened long enough for the program's auto-save feature to function, the computer system will create a temporary copy of that file in unallocated space. These temporary copies are different from normal user-created files, such as word-processing documents, which are stored on the active, or allocated, space of a computer where such information is visible to a user. As long as the file is open, a temporary copy is in unallocated space. When the file is closed (or deleted by the user), the temporary copy is not deleted. While information in unallocated space is hidden from the view of normal users, it can be recovered with the aid of technology consultants making a forensic copy. (Garrie, 2010)

Why would the operating system not completely erase a file when the user deletes it? Consider the following: If the operating system were to physically erase a file from the hard disk every time a file were deleted, it would use computing time and resources to accomplish that task depriving those resources from being used to run other active programs. Those resources would not then be available for the computer to do other productive work. The net result would be to severely slow down the processing speed of the computer. Further, it would complicate the "undelete" feature of programs. To be absolutely certain that all unallocated space were preserved, one must create a forensic image of the entire storage medium, which is not only time consuming and expensive, it could be

virtually impossible for large organizations with large and complex computer networks. In addition, for large organizations, acquiring such forensic images would necessarily mean that normal business operations would have to be suspended to capture those file fragments. To do so would be no small task, indeed. Further, it would contrary to the normal intent of a court's status quo order that would not interfere with normal, routine business operations.

RELEVANCE TO THE GENGER CASE

In the Genger case the primary dispute was over control of the Trans-Resources, Inc. (TRI) stock between the original owner of the company Arie Genger, (Genger) and new stock purchasers, known as the Trump Group. (TR Investors, LLC et. al v Genger, 2009) Originally the stockholders were Genger, his wife and children. Genger transferred some stock without the permission of the new stockholders, the Trump Group. The new investors sued Genger over the issue of who had the right to make corporate decisions. The court issued a "status quo" order while the case was being litigated. After the case was settled, Trump's computer expert discovered that wiping software had been used to erase data in the unallocated space of the computer. As a result of this discovery, Trump moved to reopen the case and sought sanctions against Genger for intentionally causing computer "wiping" software to be installed and run on his desktop computer as well as Trump's hard drives destroying information contained in the unallocated space of a server and hard drive. (TR Investors, LLC et. al v Genger, 2009)

Genger had started the company over 25 years before but also conducted non-business related activities on the company computers. He often conducted personal and consulting work on the TRI computers and conducted company business on his personal laptop. (Memorandum Opinion TR Investors, LLC, et al. v Genger, 2009). During the proceedings Genger had expressed concern that there might be stored information on his business dealings with the Israeli government and documentation concerning his personal finances and recent divorce. The fact that Genger used the TRI computers for his personal and private business use was in direct violation of the policy he set for the company's computer use. (Memorandum Opinion TR Investors, LLC, et al. v Genger, 2009). On the other hand, Trump was concerned that Genger might abscond with TRI's trade secrets. To accommodate both parties' concerns the court appointed the law firm of Friedman Kaplan to supervise the process of Genger removing his personal items from TRI's office and to review Genger's electronic files with the purpose of identifying documents that were personal to Genger. Had the Kaplan attorneys found any personal data, Genger was allowed to encrypt the information in a manner that would ensure that the documents would be protected and not accessible to TRI. As a practical matter, since the Trump Group had not been permitted access to Genger's personal files, there would be no harm in erasing them as opposed to encrypting them.

For non-personal documents, Kaplan was to preserve those documents for use by TRI in its business and make them available for the litigation. Contrary to acceptable computer forensic practice, Kaplan attorneys opened documents and emails to review their contents without regard to the forensic consequences. A problem with this practice is that it is not forensically sound, that is, the very act of opening documents and emails may alter information in unallocated space on the computer's storage media. The proper forensic standard is to create an identical and forensically sound bit stream image of the storage medium and use that image to analyze files and emails rather than the original storage medium. It is essential to work with a forensic image of the storage medium in order to guarantee the integrity of the original ESI.

The goal of the Kaplan attorneys was to complete the process during the weekend of September 6 -7 of 2008 so that the results would be ready for the following Monday meeting between attorneys. To complete the process Kaplan hired an outside technology firm, Kraft and Kennedy, Inc. (K and K) who imaged parts of the computer system in order to have a snapshot of everything on the system to date – September 7, 2008. Kraft and Kennedy made a forensic image of the active files stored on the computer's hard disk but did not create a forensic image that included unallocated space. K and K did not complete the assignment partially because it did not understand how TRI maintained computer records or the fact that the company had a server maintained at an outside source. (Genger v. TR Investors, LLC, 2011)

There is no explanation as to why TRI or its attorneys or K and K did not make or request that a forensic image of the computers be made. Further, there is no explanation as to why no one asked for additional time to complete the task, or why K and K did not demand a data map indicating all sources of ESI before conducting the

forensic search, or acquiring a forensic image of the server's hard drives as well. There is no evidence that anyone had any questions concerning electronic data sources (Luoma & Luoma, 2010) After the Kaplan attorneys and their experts had left TRI's offices with the copies it had made of electronic files, it made no indication that Trump or Kaplan intended to conduct additional searches or acquire additional copies after the September 7 date.

Once Kaplan's attorneys and Trump representatives left, Genger's forensic expert, Ohana, informed Genger that non-encrypted copies of Genger's personal files might have been created and left on the computer and server. He also pointed out that K and K had not made a copy of that unallocated space because they had copied only the active file structure. Ohana recommended that they wipe the unallocated space on both machines immediately. On September 8, 2008 at around 1:00 a.m. Ohana ran a program called "SecureClean" with the "DeepClean option. As a result of this wiping program, the data contained in unallocated space was effectively erased without erasing any active files. Genger did not mention this action to anyone. After the case was settled and the expert for the Trump Group found that TRI's computers had the unallocated space erased, they brought a motion to the court asking that the case be reopened and that Genger be sanctioned. (Memorandum Opinion TR Investors, LLC, et al. v Genger, 2009)

In its decision the court found that Genger did not contact Kaplan, K and K, or even Genger's own attorneys before running SecureClean. Genger also did not check to see if it was allowed under the status quo order or ask the court for permission. Genger argued he had no intention of destroying evidence relevant to the lawsuit but was only trying to remove any possible data left concerning his work with the Israeli Government or his own personal data. On one hand the court stated in its Memorandum and Order that it accepted Genger's version of the facts. (Memorandum Opinion TR Investors, LLC, et al. v Genger, 2009) Yet the court also found that Genger was aware that K and K missed a large amount of information and that was the reason it ran SecureClean secretly late at night. (Memorandum Opinion TR Investors, LLC, et al. v Genger, 2009) Yet the court did not question why K and K only made copies of the active files on the TRI system and failed to image the unallocated space. K and K could have easily made a forensic image of the hard drive if they had been directed to do so or thought it was relevant at the time of their search.

The court was very concerned about the data that might have been erased in the unallocated space and found that since K and K did not image the unallocated space, it was impossible to know what was erased. The court thought it was significant that when the Kaplan attorneys opened a document long enough for the auto-save feature to save a draft of a document, the computer system would have created a copy of the file on Genger's computer in unallocated space. When the user closed the computer these temporary files would leave a copy of the file in the unallocated space of the machine's hard drive that is invisible to the user. (Memorandum Opinion TR Investors, LLC, et al. v Genger, 2009)

Even with the independent consultants' conclusions the court found that other files besides personal files could have been created in the unallocated space prior to the court's status quo order. (Memorandum Opionion TR Investors, LLC, et al. v Genger, 2009) There was no evidence or testimony that there was anything significant or unique contained in the unallocated space. After a two-day hearing, the Court found Genger in contempt because he had caused potential evidence to be intentionally destroyed. The court found that Genger's actions were inappropriate and sanctioned Genger by increasing his burden of proof, requiring him to provide corroborating evidence at trial (beyond just his own testimony), requiring him to produce certain documents to the plaintiffs that he had claimed were privileged, and awarding attorney fees of $750,000 and fines of 3.2 million. (Genger v. TR Investors, LLC, 2011) This decision was later affirmed in the Delaware Supreme Court. (Genger v. TR Investors, LLC, 2011) By any standards these sanctions are severe.

The court did not lay any responsibility of the failures in this case on the Trump Group officials, their attorneys or their experts responsible for the failure to make copies of the unallocated space when they had the chance or conducting appropriate discovery. In this case the actions of Trump, their attorneys, Kaplan attorneys and their experts seemed sloppy at best and incompetent at worst. Before e-forensic discovery should have been conducted they should have requested a data map or least questioned the company's e-forensic expert for data sources. Next they should have decided what information and to what depth did they want to search forensically. If the unallocated space was important to them they should have made a mirror image of the hard drives. It is

interesting that Trump representatives never went back and attempt to do further research or request any additional e-discovery. It was just after the case was resolved that they discovered the action and wanted sanctioned to be ordered. In all other American cases from 2007 to 2011 sanctions are granted because deliberate spoliation occurs *before* or *during* the discovery process. (Luoma & Luoma, Sanctions or Safeguards: Perspective from 2007 to 2010, 2010) In the Genger case discovery was already complete with no expectation that further discovery would be required. Serious implications impacting all businesses exist if the Genger case becomes the standard for all electronic discovery practice in the future.

IMPLICATIONS AND RECOMMENDATIONS FOR BUSINESS

Based on the foregoing discussion of the Genger case, businesses will be required routinely to go to what heretofore has been considered extraordinary means to preserve all unallocated space on company computers in addition to the active ESI that now is required for electronic discovery. Businesses will need to take extra precautions to prevent the data from being overwritten. Prudent business practice would require that the issue of unallocated space to be discussed at the earliest opportunity with the opposing side and with the court. If preserving unallocated space would be a severe burden, a motion must be made to the court immediately to clarify the issue and to identify who will be responsible for the costs. For businesses of all sizes the implication is that forensic images of all storage media will need to be made no matter how many computers or storage devices are involved. This will always involve a digital forensic expert and substantial costs in expert fees, additional hardware to store the images as well as a substantial amount of time to complete the task.

The Genger case will serve as notice to all businesses that they must be prepared for litigation long before litigation is anticipated let alone begun. Further, businesses must have a retention and deletion policy in place in order to establish good faith should any ESI be deleted under normal business practice. Every employee must be educated on retention in the case of litigation or even the possibility of litigation. Data maps must be prepared identifying all types and sources of ESI. A digital forensic expert must be hired long before litigation is anticipated to join a litigation team to help establish a litigation plan, educate employees and make recommendations.

Once litigation is commenced a company must retain a digital forensic expert to help prevent inadvertently causing an act that could result in the company being subjected to sanctions from the court. The forensic expert can assist in the tasks of finding, preserving and preparing digital evidence. Preserving computer evidence comes first, even before evidence is found, because an employee can destroy ESI so easily accidentally or purposely. Additionally, as soon as litigation is anticipated the litigation hold must be in place and counsel retained.

Multi-National Enterprises (MNEs) and international companies that do business with American companies or other common law countries must consider that their organizations must constantly re-examine their electronic discovery policies, procedures, and practices, too. A digital forensic expert must be consulted regularly to be certain the company's policies are current best practices, and attorneys must be consulted to make sure the company is keeping current with the rapid change of legal rulings. Companies must plan to be proactive. Considerable expense, stress, interruption of business and loss of productivity can be prevented or at least minimized if these issues are addressed prior to litigation.

As part of the a company's retention and deletion policy a company must establish a valid business reason for periodically erasing unallocated storage space and then establia a policy that states that it routinely periodically erases unallocated space on storage devices and not wait until they are covered up in the normal course of business if they want to argue to the court that the failure to preserve unallocated space was a well-established company policy and not an act to hide data at the time of litigation. Further, companies must know where they have their ESI stored and should have a data map identifying the what, when, where, how and why there ESI is stored.

CONCLUSION

In conclusion, the opinion of these authors is that the Delaware Supreme Court's decision to affirm the trial court's imposition of sanctions against Genger was wrong. The status quo order did not indicate that the unusual practice of preserving unallocated space on Genger's computers was required. Virtually all previous cases involving

unallocated space required its preservation only if the order specifically included such a provision. Other courts have made it clear that the value of what can be obtained must be weighed against the costs of preserving and retrieving such data by applying the principle of proportionality that weighs the value received versus the cost of obtaining the information. The Trump Group in requesting sanctions had the opportunity to secure the evidence but did not, and further, did not request it at any time. The only costs the Trump Group incurred were the costs of proving that Genger had erased the unallocated space. In the authors' opinion the court should have considered shifting the costs involved to the requesting party.

From a forensics point of view, the court's requirement that unallocated should have been preserved placed an impractical and undue burden on Genger. As discussed above, the only practical way to preserve that information would have been to create a forensic image of every storage device attached to Genger's computers at substantial expense in services and additional hardware. Again, the principle of proportionality would have led to the conclusion that this requirement was unwarranted.

The final decision in this case might be unique and not be applied as a valid precedent in other courts in the future, but it cannot be dismissed and ignored by businesses determined to engage in electronic discovery best practices. If nothing else, this case stands for the idea that a clear understanding of a court's status quo order must be obtained before taking any action that could potentially be deemed to be a violation of that order. Additionally, prudent business practice requires that businesses implement the recommendations contained above in the event the Genger case becomes the canary in the coal mine for future electronic discovery practice.

AUTHOR INFORMATION

Vicki Luoma is an Associate Professor of Business Law in the Department of Accounting and Business Law at Minnesota State University in Mankato, Minnesota, and has been a member of the faculty for 8 years. Dr. Luoma teaches courses in computer and technology law, contracts, employment and labor law, and legal environment of business. Before joining MSU she practiced law for over 25 years. She received her J.D. from Salmon P. Chase College of Law at Northern Kentucky University. E-mail: Vicki.Luoma@mnsu.edu. Corresponding author.

Milton Luoma is an Assistant Professor of Information and Computer Sciences at Metropolitan State University, St. Paul, Minnesota, and has been a member of the faculty since 2002. Dr. Luoma teaches courses in digital evidence analysis, electronic discovery, and computer law in the computer forensics program as well as courses in computer science. Before joining the MSU faculty he practiced law for 25 years. He received his J.D. from William Mitchell College of Law, St. Paul, Minnesota, M.S. in Computer Science at the University of Minnesota, Duluth, and M.B.A. and M.S. in Engineering at the University of Dayton, Dayton, Ohio. E-mail: Milt.Luoma@metrostate.edu

Penny Herickhoff is a Professor of Business Law in the Department of Accounting and Business Law at Minnesota State University in Mankato, Minnesota, and has been a member of the faculty for 25 years. Dr. Herickhoff teaches courses in regulatory law, employment law and conflict management. Her primary research areas are technology law, regulatory law and conflict management. Before joining MSU, Professor Herickhoff practiced law for ten years with the firm of Farrish, Johnson, Maschka and Hottinger. Dr. Herickhoff received her J.D. and L.L.M. in Taxation from William Mitchell College of Law, St Paul, Minnesota. E-mail: Penny.Herickhoff@mnsu.edu

REFERENCES

1. Memorandum Opionion TR Investors, LLC, et al. v Genger, 3994-VCS (Chancellor 2009 йил 9-December).
2. Brady, K. a. (2010). Practitioner Note: Recent Key Delaware Corporate And Commercial Decisions. *New York University Journal of Law & Business* , 421.
3. Garrie, D. a. (2010 йил October). Legally Correct But Technologically Off the Mark. *Northwestern University, School of Law* , 1.
4. Genger v. TR Investors, LLC, WL 2802832 (Del 2011 йил 18-July).
5. Luoma, M., & Luoma, V. (2010). Data Maps and Rule 26 (f).

6. Luoma, M., & Luoma, V. (2010). Sanctions or Safeguards: Perspective from 2007 to 2010. *Southern Academy of Legal Studies in Business* (pp. 23-8). San Antonio: SALSB.
7. Memorandum Opinion TR Investors, LLC, et al. v Genger, 3994-VCS (Chancellor 2009 йил 9-December).
8. Sedona Conference. (2007). The Sedona Principles: Second Edition Best Practices Recommendations and Addressing Electronic Document Production. Sedona: Sedona Conference.
9. TR Investors, LLC et. al v Genger, WL4696062 (C.A. 2009).

NOTES